Lecture Notes

for

Elementary Set Theory

Part I

Textbook By
Richard P. Millspaugh
University of North Dakota

Lecture Notes Prepared By
Bryce A. Christopherson
University of North Dakota

Lecture Notes for Elementary Set Theory

Chapter 1

Elementary Logic

1.1 Propositions

Definition 1.1. A *proposition* is a statement that is either true or false, but not both. The *truth value* of a proposition is true (T) if the sentence is true and false (F) if the sentence is false.

Example 1.2. *Determine whether the following are propositions:*

- Two plus two equals four.
  This sentence is true, hence a proposition.
- Seven minus three equals twelve.
  This sentence is false, hence a proposition.
- It will snow in Grand Forks on March 17, 2525.
  This sentence is a proposition, we just don't happen to know the truth value.
- Go clean your room.
  This sentence is a command, not a proposition.
- Is it raining outside?
  This sentence is not a proposition. It is a question.
- This sentence is false.
  This sentence is not a proposition because it cannot be either true or false. If it is true, then it's claim is false. If it's false, then it's claim must be true.
- $x + 3 = 12$.
  This sentence cannot be said to be true or false without more information. If $x = 0$, then it is false. If $x = 9$, then it is true. Statements like this are not propositions.

We will use uppercase letters, frequently P or Q, to stand for variable propositions in much the same way that you might use x or y to represent variable numbers in algebra.

1.2

Connectives and Truth Tables

Many of the propositions we are interested in are made up of more elementary propositions. For example, the proposition S: *today is Tuesday and it's raining* is made up of the two propositions P: *today is Tuesday* and Q: *it's raining*. The word *and* in S is called a connective since it gives us a way to connect two propositions and form another. In this section we will look at several kinds of connectives.

1.2.1 Conjunction

Definition 1.3. The *conjunction* , denoted $P \wedge Q$. The conjunction $P \wedge Q$ is true when both P and Q are true and false if either P or Q (or both) are false.

We will sometimes keep track of the truth values , where we list the truth values of a propositions in terms of the truth values of elementary propositions.

Example 1.4. *Construct a truth table for the conjunction* $P \wedge Q$.

P	Q	$P \wedge Q$
T	*T*	*T*
T	*F*	*F*
F	*T*	*F*
F	*F*	*F*

Note that in this case there are four rows in the table. For a proposition made up of n elementary propositions, there will be 2^n rows in the truth table because there are two possible truth values for each of the elementary propositions. This makes it cumbersome to construct truth tables for very complicated propositions. Nevertheless, we will find them to be a convenient tool.

1.2.2 Disjunction

We next consider propositions of the form P *or* Q. We have to be a bit more careful defining what we mean in this case, because the word *or* can be ambiguous in english. That is, sometimes *or* is inclusive in the sense that it includes the possibility that both conditions are met while, other times, we presume that only one of the two options is possible. We do not want to allow this kind of ambiguity in logical propositions, so we always use the word *or* in the inclusive sense. In other words, $P \vee Q$ is true if at least one of P or Q is true.

Definition 1.5. The *disjunction*, denoted $P \vee Q$, which is true whenever at least one of P or Q is true.

Example 1.6. *Construct a truth table for the proposition* $P \vee Q$.

P	Q	$P \vee Q$
T	*T*	*T*
T	*F*	*T*
F	*T*	*T*
F	*F*	*F*

1.2.3 Implication

Most mathematical propositions have the form *If* P, *then* Q. Of course, either of P or Q might be propositions made of several other propositions.

Definition 1.7. The proposition *If* P, *then* Q is called an *implication* The implication is false only when P is true and Q is false.

Example 1.8. *Construct a truth table for* $P \Rightarrow Q$.

P	Q	$P \Rightarrow Q$
T	*T*	*T*
T	*F*	*F*
F	*T*	*T*
F	*F*	*T*

Notice: To say that $P \Rightarrow Q$ is true **does not** mean that P is true or that Q is true. It **does** mean that there is a relationship between the truth values of these two propositions. The implication $P \Rightarrow Q$ is false when P is true and Q is false; it is true when either P is false or Q is true.

There are several other implications related to the implication $P \Rightarrow Q$ that we will occasionally find useful.

Definition 1.9. For the implication $P \Rightarrow Q$:

- The *converse* is $Q \Rightarrow P$.
- The *contrapositive* is $\neg Q \Rightarrow \neg P$.
- The *inverse* of is $\neg P \Rightarrow \neg Q$.

1.2.4 Logical Equivalence

Definition 1.10. Two propositions P and Q are said to be *logically equivalent* if they always have the same truth value. We use the connective *iff*, read "if and only if," and use the symbol $\Leftrightarrow$. The proposition $P \Leftrightarrow Q$ is true when P and Q have the same truth value.

Example 1.11. *Construct a truth table for* $P \Leftrightarrow Q$.

P	Q	$P \Leftrightarrow Q$
T	*T*	*T*
T	*F*	*F*
F	*T*	*F*
F	*F*	*T*

1.2.5 Negation

Definition 1.12. The *negation* of P, denoted $\neg P$ and sometimes read "not P," is the proposition whose truth value is always opposite that of P.

Note that negation is not actually a connective since it applies to a single proposition rather than connecting two propositions.

Example 1.13. *Construct a truth table for* P *and* $\neg P$.

P	$\neg P$
T	*F*
F	*T*

1.2.6 Tautology and Contradiction

Definition 1.14. A *tautology* is a proposition that is always true, regardless of the truth values of the elementary propositions that make it up.

Definition 1.15. A *contradiction* is a proposition that is always false.

Example 1.16. *Show the proposition* $P \vee \neg P$ *is a tautology and that the proposition* $P \wedge \neg P$ *is a contradiction using a truth table.*

P	$\neg P$	$P \vee \neg P$	$P \wedge \neg P$
T	*F*	*T*	*F*
F	*T*	*T*	*F*

EXAMPLE 1.17. *Use a truth table to show that* $P \Rightarrow (P \vee Q)$ *is a tautology.*

We must construct a truth table with a column for $P \Rightarrow (P \vee Q)$ *and show that the truth values in that column are all T.*

P	Q	$P \vee Q$	$P \Rightarrow (P \vee Q)$
T	*T*	*T*	*T*
T	*F*	*T*	*T*
F	*T*	*T*	*T*
F	*F*	*F*	*T*

EXAMPLE 1.18. *Use a truth table to show that* $(P \Rightarrow Q) \Leftrightarrow (\neg Q \Rightarrow \neg P)$ *is a tautology.*

Note that we can either construct a truth table with a column for the desired equivalence and show that the truth values are all T, or we can construct a truth table with the columns for $P \Rightarrow Q$ *and* $\neg Q \Rightarrow \neg P$ *and show that the truth values are always equal to each other. We will do the latter since it is less work.*

P	Q	$\neg P$	$\neg Q$	$P \Rightarrow Q$	$\neg Q \Rightarrow \neg P$
T	*T*	*F*	*F*	*T*	*T*
T	*F*	*F*	*T*	*F*	*F*
F	*T*	*T*	*F*	*T*	*T*
F	*F*	*T*	*T*	*T*	*T*

1.3 Predicates, Instantiation, and Quantification

We return our attention now to statements that involve variables, like $x + 3 = 12$. Such a statement is called a *predicate* and we will usually indicate it with $P(x)$ rather than P. Before a predicate takes on a truth value, we need to know something about the variable. We noted before that if $x = 0$, then the statement is false; but if $x = 9$, then the statement is true. What if x represents my desk? In that case the statement is complete nonsense, but you probably feel like there's something a little bit unfair about that choice for x. We see an equation and usually think that the variable must represent a number, right? The first thing you should know about any variable in a predicate is what it can represent. This is called the *universe* or the *domain of discourse*. In mathematics, we will be very explicit about what universe we are talking about.

1.3.1 Instantiation

Let's understand that in our predicate $P(x)$ from the previous paragraph, we declare that the universe is the set of real numbers. That still doesn't turn $P(x)$ into a proposition because, as noted above, $P(x)$ doesn't take on a truth value until we know which real number x indicates. One way to do this is called *instantiation*, which means choosing a particular value for the variable(s). Consider for example the sentence: *Let* $x = 2$, *then* $x + 3 = 12$. In this case the sentence is a proposition with truth value F. The other option is *quantification* of the variable(s). We will discuss two kinds of quantifiers, *universal* and *existential*. You might occasionally encounter other quantifiers, but they are not necessary.

1.3.2 Universal Quantification

Definition 1.19. A *universal quantifier* indicates that the predicate is true for all instances of the variable in the given universe. It is typically indicated by using the phrase "for every" or "for all," and can be denoted symbolically by $\forall$ in symbolic statements.

The following sentences are universally quantified propositions. Only the second is true.

- *For every real number* x, $x + 3 = 12$.
- *The square of* x *is nonnegative for all real* x.
- *The square of* x *is nonnegative for all complex* x.

1.3.3 Existential Quantification

Definition 1.20. An *existential quantifier* indicates that the predicate is true for at least one instance of the variable in the given universe. It is typically indicated by the phrase "for some" or "there exists," and can be denoted by $\exists$ in symbolic statements.

The following sentences are existentially quantified. All three of these are true.

- *There is a real number x so that $x + 3 = 12$.*
- *The square of x is nonnegative for some real x.*
- *The square of x is nonnegative for some complex x.*

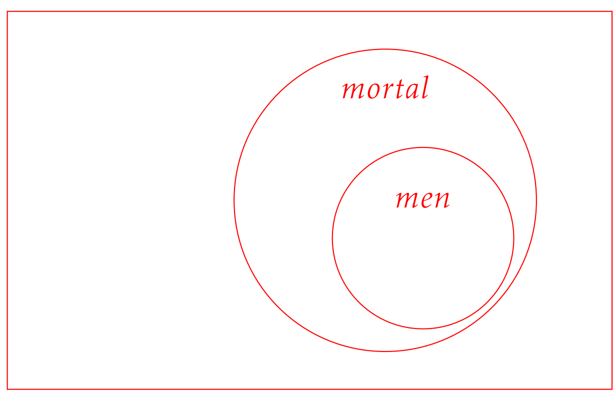
1.3.4 Syllogisms and Venn Diagrams

A *syllogism* This is a valid syllogism. If we assume that the premises are true, then the conclusion must follow.

One tool we can use to help think about syllogisms is a *Venn diagram*, which in it's simplest form is a collection of circles that represent the various categories in the premises.

Example 1.21. *Construct a Venn diagram to determine if the following syllogism is valid: All men are mortal. Socrates is a man. Hence Socrates is mortal.*

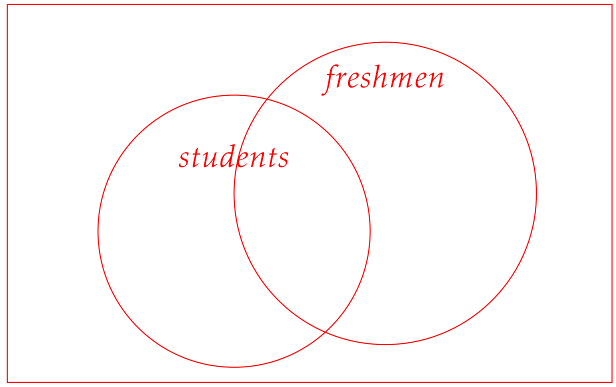
In this case we will have one circle representing mortals and another representing men. Since one of our premises is that all men are mortal, the circle representing men is completely contained inside the circle representing mortals:



Since Socrates is a man, hence inside the circle representing men, he must of necessity also be inside the circle representing mortals, hence the syllogism is valid.

Example 1.22. *Determine whether the following syllogism is valid:*
Some students are freshmen. Pat is a student. Hence Pat is a freshman.

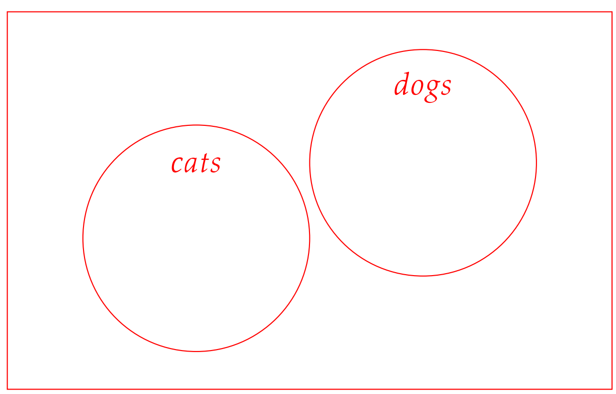
The circle for students should overlap the circle for freshmen, but need not be contained within it since our assumption is that only some students are freshmen.. Here is a Venn diagram:



Note that Pat may be in the student circle without being inside the freshmen circle, so the syllogism is not valid.

Example 1.23. *Determine whether the following syllogism is valid:*
No cats are dogs. Jade is a cat. Hence Jade is not a dog.

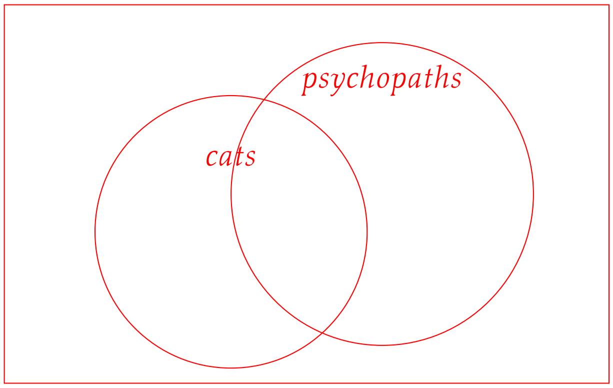
In this case, the circle for cats should be completely outside the circle for dogs since no cats are dogs. Here is a Venn diagram:



Since Jade must be within the cats circle, Jade cannot be within the dogs circle, so the syllogism is valid.

Example 1.24. *Determine whether the following syllogism is valid:*
Some cats are psychopaths. Jawa is a cat. Hence Jawa is a psychopath.

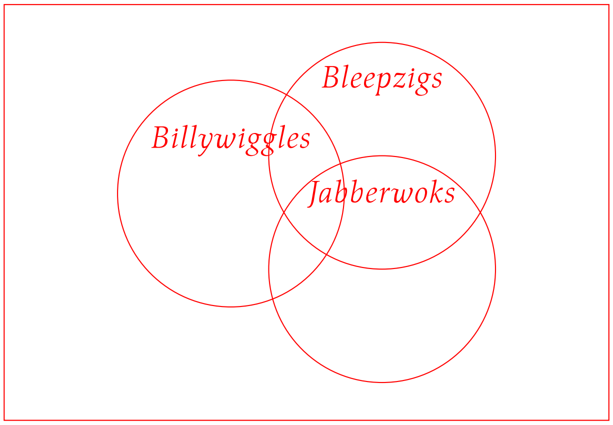
Here is a Venn diagram:

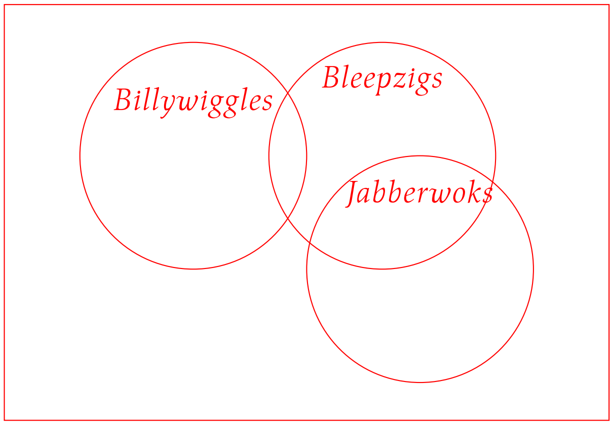


Since Jawa must be in the cats circle, but may or may not be within the psychopaths circle, this syllogism is not valid.

Example 1.25. *Determine whether the following syllogism is valid:*
Some Billywiggles are Bleepzigs. Some Bleepzigs are Jabberwoks. Hence some Billywiggles are Joabberwoks.

It is possible for the Venn diagram to look like either of the following:





This syllogism is not valid.

1.3.5 Quantification of Several Variables

A predicate can have two or more variables. In order to use the predicate in a proposition, a universe must be declared for each variable and each variable must be instantiated or quantified. We will discuss the various ways a two variable predicate might be quantified by considering an example.

Example 1.26. *Consider the predicate* $\mathrm{P}(x,y)$ *given by* $x+y=0$ *and assume that the universe for both* x *and* y *is the set of real numbers. Determine whether the following proposition is true:* $\forall x\ \forall y\ \mathrm{P}(x,y)$

This proposition can be read as for all (real) x and for all (real) y, $x+y=0$, *which says the sum of any two real numbers is 0. Clearly this is false.*

Example 1.27. *Consider the predicate* $\mathrm{P}(x,y)$ *given by* $x+y=0$ *and assume that the universe for both* x *and* y *is the set of real numbers. Determine whether the following proposition is true:* $\forall y\ \forall x\ \mathrm{P}(x,y)$.

Restating this as we did above, it is not difficult to see that this proposition is equivalent to the first one.

Example 1.28. *Consider the predicate* $\mathrm{P}(x,y)$ *given by* $x+y=0$ *and assume that the universe for both* x *and* y *is the set of real numbers. Determine whether the following proposition is true:* $\exists x\ \exists y\ \mathrm{P}(x,y)$.

We can read this as there is an x so that there is a y so that $x+y=0$, *which says that there are real numbers* x *and* y *such that* $x+y=0$. *This is true. Once again, reversing the order of the quantifiers doesn't matter.*

Example 1.29. *Consider the predicate* $P(x, y)$ *given by* $x + y = 0$ *and assume that the universe for both* x *and* y *is the set of real numbers. Determine whether the following proposition is true:* $\forall x\, \exists y\, P(x, y)$.

This proposition says that for every x there is a y such that $x + y = 0$, *in other words every real number has an additive inverse, which is certainly true.*

Example 1.30. *Consider the predicate* $P(x, y)$ *given by* $x + y = 0$ *and assume that the universe for both* x *and* y *is the set of real numbers. Determine whether the following proposition is true:* $\exists y\, \forall x\, P(x, y)$.

The variables here are quantified the same, but the order is changed. Does that matter? The proposition this time says there is a y so that for all x, $x + y = 0$. *In other words, there is some real number* y *so that adding any real number to* y *yields a sum of 0, which is certainly false!*

1.4 Negations

The negation of a proposition is the proposition with the opposite set of truth values. In this section we are going to discuss the negations of compound propositions, which can be an important step in some kinds of proofs. We begin with two theorems that tell how to find the negations of propositions involving connectives.

Theorem 1.31. *Given any propositions* P *and* Q, $\neg(P \Rightarrow Q) \Leftrightarrow (P \wedge \neg Q)$.

Proof. To see that this theorem is true, we first make sure that we understand what it is saying. The variables in this case are actually propositions P and Q, both of which are universally quantified. The theorem asserts that the compound proposition $\neg(P \Rightarrow Q) \Leftrightarrow (P \wedge \neg Q)$ is always true, so we must demonstrate that no matter what the truth values of P and Q are, the statement in the theorem is a tautology. We proceed by constructing a truth table.

P	Q	$\neg Q$	$P \Rightarrow Q$	$\neg(P \Rightarrow Q)$	$P \wedge \neg Q$
T	T	F	T	F	F
T	F	T	F	T	T
F	T	F	T	F	F
F	F	T	T	F	F

THEOREM 1.32. (DeMorgan's Laws) *Given any propositions* P *and* Q*:*

$\neg(P \wedge Q) \Leftrightarrow (\neg P \vee \neg Q)$

(ii) $\neg(P \vee Q) \Leftrightarrow (\neg P \wedge \neg Q)$

You will prove this theorem in the homework.

EXAMPLE 1.33. *Negate the proposition* $P \Rightarrow (Q \wedge R)$.

We apply what we know one step at a time, beginning with the implication:

$$\begin{aligned} \neg\big(P \Rightarrow (Q \wedge R)\big) &\Leftrightarrow P \wedge \big(\neg(Q \wedge R)\big) && \textit{(Theorem 1.31)} \\ &\Leftrightarrow P \wedge (\neg Q \vee \neg R) && \textit{(Theorem 1.32(i))} \end{aligned}$$

EXAMPLE 1.34. *Find the negation of* $P \wedge (Q \Rightarrow R)$.

We apply Theorem 1.31 and Theorem 1.32 where indicated.

$$\begin{aligned} \neg\big(P \wedge (Q \Rightarrow R)\big) &\Leftrightarrow \big(\neg P \vee \neg(Q \Rightarrow R)\big) && \textit{(Theorem 1.32(i))} \\ &\Leftrightarrow \big(\neg P \vee (Q \wedge \neg R)\big) && \textit{(Theorem 1.31} \end{aligned}$$

Example 1.35. *Find the negation of* $(P \vee Q) \wedge (P \vee R)$.

We apply Theorem 1.32 where indicated.

$$\begin{aligned} \neg\big((P \vee Q) \wedge (P \vee R)\big) &\Leftrightarrow \big(\neg(P \vee Q) \vee \neg(P \vee R)\big) && \textit{(Theorem 1.32(i))} \\ &\Leftrightarrow \big((\neg P \wedge \neg Q) \vee (\neg P \wedge \neg R)\big) && \textit{(Theorem 1.32(i,ii))} \end{aligned}$$

Chapter 2

Logical Arguments

2.1 Rules of Inference

We accept the following two basic rules of thought:

> The *Law of Excluded Middle* says that given any proposition P, we may deduce $P \vee \neg P$. In words, either P is true or $\neg P$ is true.
>
> The *Law of non-Contradiction* says that given any proposition P, we may deduce $\neg(P \wedge \neg P)$. In words, P and $\neg P$ cannot both be true.

A *rule of inference* is a logical rule consisting of a hypothesis and a conclusion. Whenever the hypothesis is true, the conclusion must also be true. For our purposes this means that once we have deduced all of the hypotheses, we may also deduce the conclusion. Rules of inference are closely related to tautologies. In fact, they are essentially the same thing. While every tautology gives rise to a rule of inference, in practice the seven listed in the table below will usually suffice.

Table 2.1: Rules of Inference

Name	**Hypotheses**	**Conclusion**
Modus ponens	P and $P \Rightarrow Q$	Q
Modus tolens	$\neg Q$ and $P \Rightarrow Q$	$\neg P$
Hypothetical syllogism	$P \Rightarrow Q$ and $Q \Rightarrow R$	$P \Rightarrow R$
Addition	P	$P \vee Q$
Simplification	$P \wedge Q$	P
Conjunction	P and Q	$P \wedge Q$
Disjunctive syllogism	$P \vee Q$ and $\neg P$	Q

The Rule of Addition, for example, comes from the tautology $P \Rightarrow (P \vee Q)$. Since the implication is always true, knowing that the hypothesis is true will tell us that the conclusion must also be true. We can verify each of the Rules of Inference in Table 2.1 by constructing a truth table for the associated tautology.

2.1.1 Propositional Arguments

Each of our Rules of Inference is actually a *propositional argument*, where accepting the hypotheses forces us to accept the conclusion. We use the following notation for propositional arguments, where the propositions above the line are hypotheses and the proposition(s) below the line are the conclusion(s). We precede the conclusions(s) with the symbol $\therefore$ which is read "therefore."

Example 2.1. *Here is the rule of modus tolens as a propositional argument:*

$$\begin{array}{ll} & \neg Q \\ & P \Rightarrow Q \\ \hline \therefore & \neg P \end{array}$$

Example 2.2. *Express the rule of modus ponens as a propositional argument.*

$$\begin{array}{ll} & P \\ & P \Rightarrow Q \\ \hline \therefore & Q \end{array}$$

Example 2.3. *Express the rule of hypothetical syllogism as a propositional argument.*

$$\begin{array}{ll} & P \Rightarrow Q \\ & Q \Rightarrow R \\ \hline \therefore & P \Rightarrow R \end{array}$$

Definition 2.4. A propositional argument is said to be *valid* if accepting the hypotheses forces us to accept the conclusion(s).

How do we determine whether or not a propositional argument is valid? One option is to construct a truth table, but that can be very tedious. Our preferred option is to construct a logical argument which begins by assuming each of the hypotheses is true and deduces consequences using our rules of inference. Each deduced proposition is a step in our proof that can be justified as either a hypothesis, a tautology, a consequence of previous steps and a rule of inference, or a proposition that is logically equivalent to a previous step. The proof is complete when we have deduced the desired conclusion.

Example 2.5. *Prove that the following argument is valid:*

$$\begin{array}{l} P \\ P \Rightarrow Q \\ \underline{(Q \vee R) \Rightarrow S} \\ \therefore\ S \end{array}$$

Proof.

(1)	P	hypothesis
(2)	$P \Rightarrow Q$	hypothesis
(3)	Q	modus ponens, (1) and (2)
(4)	$Q \vee R$	addition, (3)
(5)	$(Q \vee R) \Rightarrow S$	hypothesis
(6)	S	modus ponens, (4) and (5)

Example 2.6. *Prove that the following argument is valid:*

$$\begin{array}{l} \mathrm{P} \Rightarrow (\mathrm{Q} \wedge \neg \mathrm{Q}) \\ \hline \therefore\ \neg \mathrm{P} \end{array}$$

Proof.

(1)	$\mathrm{P} \Rightarrow (\mathrm{Q} \wedge \neg \mathrm{Q})$	hypothesis
(2)	$\neg(\mathrm{Q} \wedge \neg \mathrm{Q})$	non-Contradiction
(3)	$\neg \mathrm{P}$	modus tolens, (1) and (2)

The argument in Example 2.6 says that if a proposition P implies a contradiction, then $\neg$P must be true. This result is the basis for proofs by contradiction.

2.1.2 Arguments with Quantifiers

Arguments involving quantified propositions require us to have rules of inference for instantiation and quantification. The *rules for instantiation* when we can deduce statements about particular elements of the domain given quantified statements. The *rules for generalization* tell us when we can deduce quantified statements given deductions about particular elements of the domain. We give these rules in Table 2.2.

Table 2.2: Rules of Quantification

Name	**Rule**
Universal Instantiation	$\forall x\ \mathrm{P}(x) \therefore \mathrm{P}(c)$ whenever c is in the domain of x
Existential Instantiation	$\exists x\ \mathrm{P}(x) \therefore \mathrm{P}(c)$ for some c in the domain of x
Universal Generalization	$\mathrm{P}(c)$ for *arbitrary* c in the domain of $x \therefore \forall x\ \mathrm{P}(x)$
Existential Generalization	$\mathrm{P}(c)$ for *some* c in the domain of $x \therefore \exists x\ \mathrm{P}(x)$

Example 2.7. *Prove that the following argument is valid:*

$$\begin{array}{l} \forall x\ (\mathrm{P}(x) \wedge \mathrm{Q}(x)) \\ \underline{\exists x\ (\mathrm{P}(x) \Rightarrow \mathrm{R}(x))} \\ \therefore\ \exists x\ (\mathrm{Q}(x) \wedge \mathrm{R}(x)) \end{array}$$

Proof.

(1)	$\exists x\ (\mathrm{P}(x) \Rightarrow \mathrm{R}(x))$	hypothesis
(2)	$\mathrm{P}(c) \Rightarrow \mathrm{R}(c)$ *for some c*	existential instantiation, (1)
(3)	$\forall x\ (\mathrm{P}(x) \wedge \mathrm{Q}(x))$	hypothesis
(4)	$\mathrm{P}(c) \wedge \mathrm{Q}(c)$	universal instantiation, (3)
(5)	$\mathrm{Q}(c)$	simplification, (4)
(6)	$\mathrm{P}(c)$	simplification, (4)
(7)	$\mathrm{R}(c)$	modus ponens, (2) and (6)
(8)	$\mathrm{Q}(c) \wedge \mathrm{R}(c)$	conjunction, (5) and (7)
(9)	$\exists x\ (\mathrm{Q}(x) \wedge \mathrm{R}(x))$	existential generalization, (8)

2.2 Proving Mathematical Theorems

Most mathematical statements are implications of the form $P \Rightarrow Q$, where P or Q might be compound propositions. In this section we will look at some methods for proving implications. Note that we are using some definitions and results from other areas of mathematics that we have not explicitly stated. We will not allow ourselves to make those kinds of assumptions once we begin our study of set theory.

2.2.1 Direct Proofs

A direct proof of the implication $P \Rightarrow Q$ assumes that the hypothesis P is true, then uses definitions, previously proved theorems, and the rules of inference to deduce that the conclusion Q must also be true.

Example 2.8. *Prove the following theorem:*

Theorem 2.9. *If n is an even integer, then n^2 is even.*

Proof.

(1)	n is an even integer	hypothesis
(2)	$n = 2k$ for some integer k	definition, (1)
(3)	$n^2 = (2k)^2$	definition, (2)
(4)	$n^2 = 4k^2$	algebra, (3)
(5)	$n^2 = 2(2k^2)$	algebra, (4)
(6)	n^2 is even	definition, (5)

Although the two-column proof above is valid, it is not written in a format that mathematicians usually find pleasing. We prefer proofs that are written using complete sentences, paragraphs, and correct grammar and punctuation. Here is a better presentation for the previous proof.

Example 2.10. *Prove Theorem 2.9 in plain language.*

Proof. Let n be an even integer. By definition, $n = 2k$ for some integer k. Squaring both sides yields $n^2 = 4k^2 = 2(2k^2)$. Since $2k^2$ is an integer, the quantity $n^2 = 2(2k^2)$ is even as desired.

Example 2.11. *Prove the following theorem:*

Theorem 2.12. *The square of an odd integer is odd.*

Proof. Let n be an odd integer. By definition, $n = 2k + 1$ for some integer k. Squaring both sides yields $n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$. Since $2k^2 + 2k$ is an integer, the quantity $n^2 = 2(2k^2 + 2k) + 1$ is odd as desired.

2.2.2 Proving the Contrapositive

As you have shown in a homework exercise, the contrapositive of an implication is logically equivalent to the implication. Sometimes it is easier to prove the contrapositive of the implication we are interested in, as we will show here.

Example 2.13. *Prove the following theorem:*

Theorem 2.14. *If n is an integer and n^2 is even, then n is even.*

Proof. We might try to begin this proof as we did the proof of Theorem 2.9. First assume that n^2 is even. By definition we know that $n^2 = 2k$ for some integer k. Now what? In the previous example we were able to square $2k$ and see that the result was even, but taking the square root doesn't tell us anything useful. Instead we prove the contrapositive of the theorem: *If n is an integer that is not even, then n^2 is not even.* We use the fact that every integer is either even or odd, but never both.

(1)	assume n is not an even integer	hypothesis
(2)	n is an odd integer	theorem
(3)	n^2 is odd	Theorem 2.12
(4)	if n is even, n^2 is even	Theorem 2.9
(5)	n is not even	modus tolens, (3) and (4)
(6)	n is odd	theorem

Example 2.15. *Prove the following theorem:*

Theorem 2.16. *If n is an integer and n^2 is odd, then n is odd.*

Proof. We prove the contrapositive of the theorem: *If n is an integer that is not odd, then n^2 is not odd.* Again, we use the fact that every integer is either even or odd, but never both.

(1)	assume n is not an odd integer	hypothesis
(2)	n is an even integer	theorem
(3)	n^2 is even	Theorem 2.9
(4)	if n is odd, n^2 is odd	Theorem 2.9
(5)	n is not odd	modus tolens, (3) and (4)
(6)	n is even	theorem

2.2.3 Proof by Contradiction

A proof by contradiction, or *reductio ad absurdum*, begins by assuming that the result we are trying to prove is false, then deriving a contradiction from that assumption. It is easy to confuse this with a direct proof of the contrapositive, which makes different beginning assumptions. To prove the implication $P \Rightarrow Q$ by proving the contrapositive, you assume $\neg Q$ and use that to prove $\neg P$. A proof by contradiction assumes $P \wedge \neg Q$ and derives a contradiction $R \wedge \neg R$. Here is a classic example of a proof by contradiction.

Example 2.17. *Prove the following theorem:*

Theorem 2.18. *There is no rational number x such that $x^2 = 2$.*

Proof. Suppose to the contrary that there is a rational number x with $x^2 = 2$. Since x is rational, we may express x as a fraction p/q in lowest terms, in other words p and q are integers and no integer evenly divides both of them. Since $x = p/q$ and $x^2 = 2$, we have $p^2/q^2 = 2$, or:

$$p^2 = 2q^2 \tag{2.1}$$

Since q^2 is an integer, $p^2 = 2q^2$ is even. Now p is an integer and p^2 is even, so Theorem 2.14 implies that p is even. This allows us to write $p = 2k$ for some integer k. We plug this into Equation (2.1) to see that $4k^2 = 2q^2$, so $q^2 = 2k^2$. Now q is an integer and q^2 is even, so another application of Theorem 2.14 implies that q is even. We now know that both p and q are even, so 2 divides both of them. This contradicts our choice of p and q, so our assumption that x is rational must be incorrect.

2.2.4 Proof by Cases

To prove the implication $P \Rightarrow Q$ by cases, we make use of the following argument:

$$\begin{array}{l} P \Rightarrow (R \vee S) \\ R \Rightarrow Q \\ \underline{S \Rightarrow Q} \\ \therefore\ P \Rightarrow Q \end{array}$$

You will be asked to show that this argument is valid in the homework.

Here is a very simple example of a proof by cases. We make use of some of the order properties of the real numbers. In particular, we know that multiplying both sides of an inequality by a positive number preserves the inequality, and multiplying both sides of an inequality by a negative number reverses the inequality.

Example 2.19. *Prove the following theorem:*

Theorem 2.20. *If x is a real number, then $x^2 \geq 0$.*

Proof. If x is a real number, then either $x \geq 0$ or $x < 0$.

Case 1. If $x \geq 0$, then we may multiply both sides of this inequality by x to see that $x^2 \geq x \cdot 0 = 0$.

Case 2. If $x < 0$, then muliplying both sides of the inequality by x reverses the inequality, yielding $x^2 > x \cdot 0 = 0$. Since $x^2 > 0$ we have $x^2 \geq 0$.

In either case we have $x^2 \geq 0$, so the result is true.

2.3 Proving Quantified Statements

2.3.1 Universally Quantified Statements

On the simplest level, a universally quantified statement has the form $\forall x\ P(x)$. To prove such a proposition, we assume that x is in the required domain and show that $P(x)$ must be true. It is frequently helpful to think of such a statement as an implication where the hypothesis is that x is in the required domain, and the conclusion is $P(x)$. Since universally quantified statements can be thought of as implications, we can use the same proof techniques.

2.3.2 Existentially Quantified Statements

Existentially quantified statements are significantly different than implications and universally quantified statements. To prove the statement $\exists x, P(x)$ we must show that there is at least one x in the domain that satisfies $P(x)$. One way to do this is simply to find a single particular example.

Example 2.21. *Prove the following theorem:*

Theorem 2.22. *There is a positive integer* N *such that* N, $N+1$, $N+2$, $N+3$, *and* $N+4$ *are all composite (not prime).*

Proof. Let $N = 6! + 2$. Clearly, N is divisible by 2. Likewise, $N+1 = 6!+3$ is divisible by 3, $N+2 = 6!+4$ is divisible by 4, $N+3 = 6!+5$ is divisible by 5, and $N+4 = 6!+6$ is divisible by 6.

There are some instances where it is easier to show that some x satisfies $P(x)$ without actually finding a particular x that works. Here is an elementary example that works by demonstrating that one of two possible choices must work, without determining which it is.

Example 2.23. *Prove the following theorem:*

Theorem 2.24. *There exist irrational numbers a and b so that a^b is rational.*

Proof. First note that $\sqrt{2}$ is irrational, but

$$\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\sqrt{2}} = \sqrt{2}^{\,2} = 2$$

is rational. Now it is certainly true that $\sqrt{2}^{\sqrt{2}}$ is either rational or irrational. If $\sqrt{2}^{\sqrt{2}}$ is rational, then we set $a = \sqrt{2}$ and $b = \sqrt{2}$ to find the example we need. If $\sqrt{2}^{\sqrt{2}}$ is irrational, then we set $a = \sqrt{2}^{\sqrt{2}}$ and $b = \sqrt{2}$ to find the example we need. Either way, there are irrational numbers a and b such that a^b is rational.

2.3.3 Counterexamples.

An example showing that a universally quantified statement is false is called a *counterexample* to that statement.

Example 2.25. *Disprove the following proposition:*

Conjecture 2.26. *Every integer is even.*

It probably seems clear to you that this statement is false, but how could you prove that? To prove that a proposition is false we must prove that it's negation is true, so we first find the negation of the original statement:

Some integer is not even.

We have transformed our original problem (proving that a statement is false) into something more familiar (proving that a statement is true). How do we prove the second statement is true? As noted above, one way to prove an existentially quantified statement is simply to find the object it says exists. In this case, we must find an integer that is not even. For instance, the integer $x = 1$ is not even. Note that you shouldn't just say that there are such examples, you should give a particular one that your reader can check.

2.4

Mathematical Induction

There is another type of proof that is frequently used to prove statements about the natural numbers, i.e. the numbers $1, 2, 3, \ldots$.

Theorem 2.27 (The Principle of Mathematical Induction). *Let* $\mathrm{P}(n)$ *be a statement about the natural number* n. *If* $\mathrm{P}(1)$ *is true and if* $\mathrm{P}(k) \implies \mathrm{P}(k+1)$ *for every natural number* k, *then* $\mathrm{P}(n)$ *is true for every natural number* n.

All proofs by induction use the following basic outline. To prove $\mathrm{P}(n)$ for all natural numbers n,

(i) Base Case: Show that $\mathrm{P}(1)$ is true.

(ii) Inductive Step: Prove the implication $\mathrm{P}(k) \implies \mathrm{P}(k+1)$ for all $k \in \mathbb{N}$. Note: in proving that $\mathrm{P}(k) \implies \mathrm{P}(k+1)$, the assumption that $\mathrm{P}(k)$ is true is often referred to as the inductive hypothesis.

(iii) It is considered good form to clearly state that the statement $\mathrm{P}(n)$ is now true for all natural numbers n by induction.

Example 2.28. *Prove the following theorem:*

Theorem 2.29. *For each natural number n, $\displaystyle\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.*

Proof. If $n = 1$, then
$$\sum_{i=1}^{n} i = \sum_{i=1}^{1} i = 1 = \frac{1(2)}{2} = \frac{n(n+1)}{2}.$$
So, the formula holds for $n = 1$. Now suppose that the formula holds for some $k \in \mathbb{N}$. In other words, we are assuming that $\displaystyle\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$. We want to show that the formula must hold for $n = k + 1$. Using our assumption, we compute:

$$\begin{aligned}
\sum_{i=1}^{k+1} i &= \left(\sum_{i=1}^{k} i\right) + (k+1) \\
&= \frac{k(k+1)}{2} + (k+1) \\
&= \frac{k(k+1)}{2} + \frac{2(k+1)}{2} \\
&= \frac{(k+1)(k+2)}{2}
\end{aligned}$$

Hence the formula holds for $n = k + 1$. By induction, the formula must hold for all $n \in \mathbb{N}$.